



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/404,712	09/24/1999	KOJI MANABE	040373-0263	8708

7590 07/31/2003

FOLEY & LARDNER
3000 K STREET NW
SUITE 500
WASHINGTON, DC 25696

EXAMINER

KLIMACH, PAULA W

ART UNIT

PAPER NUMBER

2131

DATE MAILED: 07/31/2003

✓

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/404,712	MANABE, KOJI
	Examiner Paula W Klimach	Art Unit 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 31 October 2002.

2a) This action is FINAL. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-7 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-7 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11) The proposed drawing correction filed on _____ is: a) approved b) disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12) The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All b) Some * c) None of:

1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) The translation of the foreign language provisional application has been received.

15) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) Notice of References Cited (PTO-892)

2) Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) Information Disclosure Statement(s) (PTO-1449) Paper No(s) 5 .

4) Interview Summary (PTO-413) Paper No(s) _____.

5) Notice of Informal Patent Application (PTO-152)

6) Other: _____

DETAILED ACTION

Priority

1. Should applicant desire to obtain the benefit of foreign priority under 35 U.S.C. 119(a)-(d) prior to declaration of an interference, a translation of the foreign application should be submitted under 37 CFR 1.55 in reply to this action.

Specification

2. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

The following title is suggested: "Digital Video and Audio Data Encryption, Decryption and System Authentication".

Claim Rejections - 35 USC § 103

3. **Claims 1-5** are rejected under 35 U.S.C. 103(a) as being unpatentable over Murphy (5,640,452) in view of Heer et al (6,028,933), Kazuyoshi (JP 0 9035030 A), and He (944,824).
4. *In reference to claims 1, 2, and 3*, Murphy discloses a system for audio and video decryption, which suggests an AV data transmitting-receiving device comprises command input means, command control means, AV data transmitting means, encrypting means (Fig. 1); a transmitting-receiving device on another party comprises second input/output means, AV data receiving means, decrypting means (column 7 lines 21-32), device ID detecting means (column 6 lines 41-50).

However Murphy does not disclose the authentication of the devices and the maintenance of an authentication history.

Kazuyoshi discloses a fourth memory (34) stores the authentication log. An access controller (4) permits the access for every command when the authentication log containing the authentication demand from command execution part satisfies the access control data (basic abstract). The authentication log keeps a history that authentication has been previously performed.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to maintain a history log of authentication as taught by Kazuyoshi for a system disclosed by Murphy. One of ordinary skill in the art would have been motivated to do this because it improves security of accessing IC card (page 2 paragraph 2).

Heer teaches authenticating means performs a device authentication operation for mutually checking that both said devices (Heer et al 6,028,933 Fig. 25), a key exchange operation for sharing a cryptographic key (Heer Fig. 24), and a cryptographic key storing means (column 26 lines 52-58).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the teachings of Heer of mutual authentication and key exchange in the combination of Murphy and Kazuyoshi. One of ordinary skill in the art would have been motivated to do this because it creates a hierarchical flow of trust via public certificates

He discloses authentication based on certain rules, access list (column 5 lines 15-26). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to authenticate using rules, access list, as disclosed by He in the combination of Murphy, Heer, and Kazuyoshi. One of ordinary skill in the art would have been motivated to do this because The user 12 can simply choose from the list the desired network element 20 and is not

even aware of the existence of the Network Elements 20 that the user 12 is not authorized to access

5. *In reference to claim 4, the system disclosed by Murphy comprises the steps of detecting an ID of said transmitting-receiving device on another party with said, device ID detecting means (Murphy column 6 lines 41-48). Notifying command to said AV data transmitting means through said command control means and starting transmission of the AV data with said AV data transmitting means, when a command input for an AV data transmission direction is provided from a user to said command input means (Murphy column 7 lines 21-29). Murphy suggests waiting for a command input for an AV data transmission direction from a user to said command input means, if the ID of said transmitting-receiving device on another party is not included in the historical information (Fig. 1). Murphy further suggests notifying the command to said AV data transmitting means through said command control means and starting transmission of the AV data with said AV data transmitting means (Fig. 1); encrypting the AV data with said encrypting means using the cryptographic key and sending the encrypted AV data to said first input/output means; sending the encrypted AV data to a transmission line with said first, input/output means (Murphy column 7 lines 34-49); receiving the encrypted AV data from the transmission line with said second input/output means (Murphy Fig. 2). The Murphy system decrypts the encrypted AV data with said decrypting means using the cryptographic key and sending the decrypted AV data to said AV data receiving means; and receiving the decrypted AV data with said AV data receiving means (Fig. 3).*

Kazuyoshi discloses checking whether the of said transmitting receiving device on another party is included in historical information stored in said authentication histories storing means

(Kazuyoshi basic abstract); access is allowed if authentication log contains the authentication demand that satisfies the access control data and Heer performs a key exchange, which is a method of mutual authentication. Kazuyoshi implies recording the ID of said transmitting receiving device on another party as historical information in said authentication histories storing means after the device authentication and the key exchange operations (Kazuyoshi basic-abstract). The Kazuyoshi authentication history (log) is used to determine if authentication demand was made followed Heer key exchanged is used to encrypt and decrypt, but is also a method of mutual authentication and therefore a form of authentication.

Performing the device authentication operation and the key exchange operation with said second authenticating means on another party by said first authenticating means is disclosed by Heer (Fig. 25). The ID of said transmitting-receiving device on another party is included in the historical information as suggested by Kazuyoshi. Heer discusses performing the device authentication operation and the key exchange operation with said second authenticating means on another party by said first authenticating means, which can be carried out when the command input for the AV data transmission direction is provided by the transmission of Murphy in Fig. 1 (Heer Fig. 25).

6. *In reference to claim 5*, in addition to the limitations discussed for claim 4, Heer records a cryptographic key shared as a result of the key exchange operation as a first cryptographic key in said cryptographic key storing means (column 26 lines 52-58 in combination with claim 3).

7. **Claims 6 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Murphy, He, Kazuyoshi, and Heer as applied to claims 4 and 5 respectively above, and further in view of Kunzman.**

The combination of Murphy, He, Kazuyoshi, and Heer do not disclose the use of the IEEE 1394 serial bus.

Kunzman teaches the use of IEEE 1394 for real-time data transport (page 406 paragraph 3).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the IEEE 1394 serial bus for the transportation of audio visual data in the combination of Murphy, He, Kazuyoshi, and Heer. One of ordinary skill in the art would have been motivated to do this because it provides an ideal mechanism for connection digital consumer audio/video equipment (summary).

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Murphy	5,640,452
Heer et al	6,028,933
Kazuyoshi	JP 0 9035030 A
He	944,824
Kunzman	IEEE 1394 High Performance Serial Bus The Digital Interface for ATV

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W Klimach whose telephone number is (703) 305-8421. The examiner can normally be reached on Mon to Fri 7:15 a.m to 3:45 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 305-8421 for regular communications and (703) 305-8421 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-4832.

PWK
July 25, 2003


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100